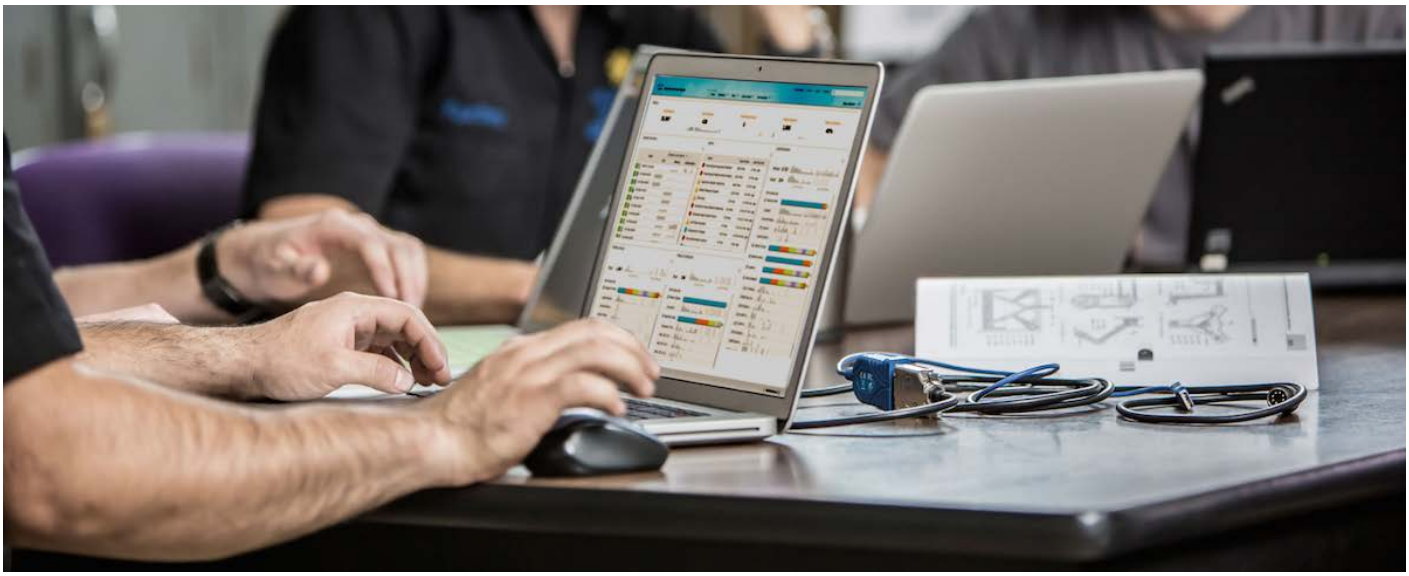

Cisco Identity Services Engine 1.2의 게스트 웹 포털 사용자 지정

보안 액세스 방법 가이드 시리즈

날짜: **2014년 12월 18일**

저자: **Cisco Identity Services Engine** 기술 마케팅 엔지니어 **Imran Bashir, Jason Kunst, Hsing-Tsu Lai**

목차

소개

이 해결책에서는 게스트가 속한 AD 그룹에 따라 달라지는 사용자 지정 성공 페이지를 표시하는 방법을 소개합니다.

활용 사례

이번 요구 사항에서는 Apple 및 Microsoft 업체 직원이 방문하기 때문에 각 업체 직원 유형에 따라 사용자 지정 ISE 웹 인증 성공 페이지를 제공하려 합니다.

추가 정보:

- 회사 네트워크에 연결된 서로 다른 2개 업체의 직원. 예: Apple_Contractor, Microsoft_Contractor.
- 이 업체 직원은 각자의 Active Directory 인증서를 사용하여 중앙 집중식 웹 인증(게스트 포털)에 로그인하는 방법으로 네트워크에 연결합니다.
- 업체 직원이 웹 인증(게스트) 포털에 로그인했으면 로그인한 그룹에 따라 다음과 같습니다.
  - Apple 업체 직원에게는 Apple 사용자 지정 성공 페이지가 표시되어야 합니다.
  - Microsoft 업체 직원에게는 Microsoft 사용자 지정 성공 페이지가 표시되어야 합니다.

문제

ISE에서 성공 페이지는 게스트 포털에 하드코딩되어 있습니다. 따라서 로그인 플로우에서 단 하나의 구성된 포털을 사용한다면 AD 그룹에 따라 각기 다른 성공 페이지를 표시할 수 없습니다.

해결책

디바이스 등록 웹 인증 플로우를 활용하여 AD 인증서에 따라 사용자 지정 성공 페이지 표시

주의사항

- 엔드포인트 그룹을 삭제하는 방법이 없으므로 직접 지워야 합니다. ISE 1.3은 엔드포인트 그룹별 자동 지우기 기능이 있습니다.
- 1.3으로 업그레이드한 후에는 포털 플로우 및 구 방식에 큰 변화가 있으므로 이 방법이 유효하지 않을 것입니다. 업그레이드할 계획이라면 업그레이드 이후에 시스템이 어떻게 작동할지 검증하는 것이 좋습니다.
- ISE 1.3에서는 이 사용자 지정을 다르게 처리하므로 이 문서에 적용되지 않습니다.

일반적으로 새로운 해결책은 테스트 환경에서 시험하고 검증한 후에 프로덕션 환경에 적용하는 것이 좋습니다.

컨피그레이션 단계

본 컨피그레이션 문서에서는 사용자가 ISE 1.2 인증 및 권한 부여 정책에 게스트 액세스를 구성한 경험이 있다고 가정합니다. 이 작업에 필요한 화면 및 최소 단계를 살펴보겠습니다.

엔드포인트 그룹 생성

업체 직원(방문자) 유형별로 필요한 엔드포인트 그룹을 만듭니다.

1단계 업체 직원 엔드포인트를 위해 2개의 엔드포인트 ID 그룹을 만듭니다. MAC 주소는 DRW 포털에 리디렉션된 다음에 등록됩니다.

2단계 **Administration > Groups > Endpoint Identity Groups**로 이동합니다.

3단계 다음 엔드포인트 그룹을 추가합니다.

- **Apple_Contractor** = Apple 업체 직원을 위한 엔드포인트 ID 그룹
- **Microsoft_Contractor** = Microsoft 업체 직원을 위한 엔드포인트 ID 그룹

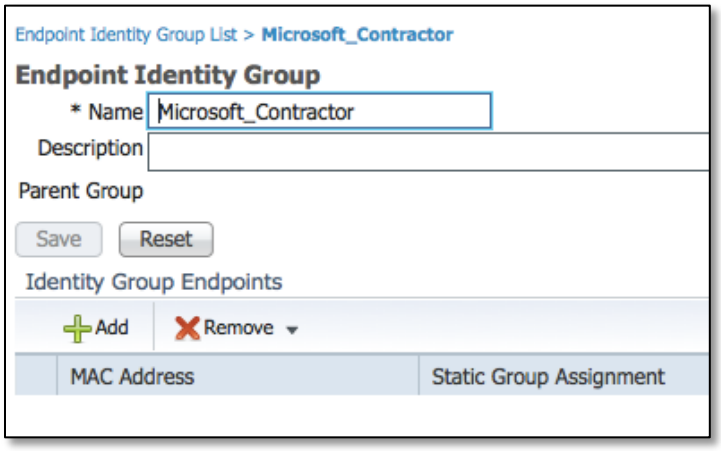

그림 1. 엔드 포인트 ID 그룹

4단계 3개의 사용자 지정 게스트 포털을 만듭니다.

- 리디렉션을 트리거할 성공 페이지 타이머를 포함한 CWA 로그인용 사용자 지정 포털입니다.
- 해당 엔드포인트 ID 그룹에 MAC 주소를 삽입할 DRW 페이지(업체 직원 유형별로 하나씩)입니다.

직접 사용자 지정 포털 페이지를 만드는 방법에 대해서는 ISE12 웹 포털 사용자 지정 방법 링크를 참조하십시오.

기본 포털 및 업체 직원 포털 생성

1차 포털 = Default_Custom

1단계 **Administration > Settings > Guest > Multi-Portal Configurations**로 이동합니다.

1차 포털 = Default_Custom

Open SSID(MAB)에 연결되는 모든 엔드포인트가 CWA의 결과로 리디렉션되는 기본 포털입니다.

성공 페이지는 3초가 지나면 어떤 URL(사용자의 리디렉션 ACL에서는 차단됨)로 리디렉션되도록 설정되었습니다.

이 코드의 예:

2단계 HTML 코드의 <HEAD> 태그와 </HEAD> 태그의 사이에 다음 HTML 리디렉션 코드를 넣습니다.

```
<meta HTTP-EQUIV="REFRESH" content="3" url="http://www.yahoo.com">

The above HTML redirect code will redirect your visitors to another web page instantly.
The content="3" is the time in seconds before redirection takes place. Don't set it lower then
this value as this is required to be longer than the COA time.
```

3단계 사용할 업로드된 파일을 매핑합니다. 적어도 로그인, 성공, 오류 페이지가 필요합니다.

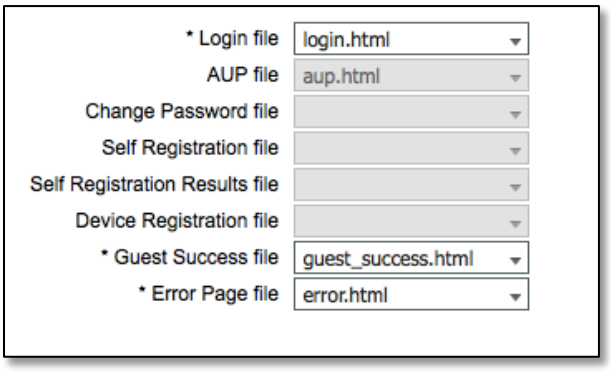

그림 2. 로그인 파일

2차 포털 = APPLE_DRW

4단계 업체 직원 유형별로 포털을 만듭니다. 그 단계는 모든 업체 직원 유형에서 동일합니다.

이것은 사용자 지정 DRW 포털입니다. 이 포털에서는 Apple 업체 직원의 디바이스 MAC 주소를 엔드포인트 ID 그룹 = Apple_Contractor에 넣습니다.

Apple 업체 직원을 위한 메시지로 이 페이지를 사용자 지정해야 합니다.

예: Welcome Apple! Here is the apple info

앞서 사용한 방법 가이드를 참조하여 이 페이지를 만들 수 있습니다. 동일한 유형입니다.

5단계 **AUP를 비활성화**합니다. Guest users should agree to an acceptable use policy 확인란을 선택 취소하면 됩니다.

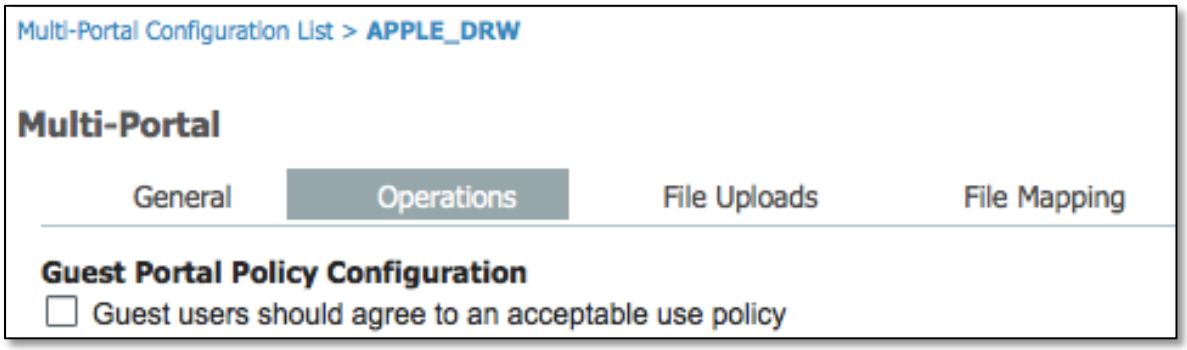

그림 3. Multi-Portal Configuration List > Apple_DRW

6단계 성공 및 오류 페이지 요구 사항에 따라 사용자 지정하고 매핑해야 합니다.
7단계 업로드된 파일을 **매핑**합니다.

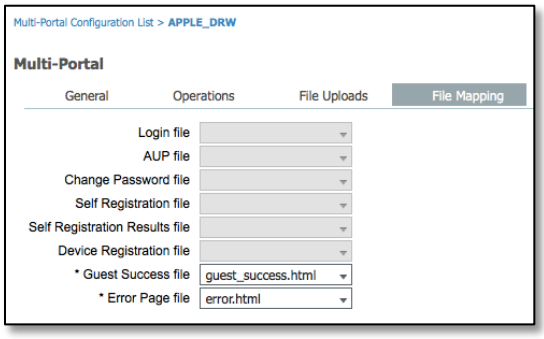

그림 4. Multi-Portal Configuration List > Apple_DRW - Error Page

다른 업체 직원 유형을 위한 포털을 만들려면 위와 동일한 단계를 수행합니다.

3차 포털 = MICROSOFT_DRW

인증 정책 생성

MAB(MAC Authentication Bypass)의 결과로 리디렉션하기 위한 인증 정책을 생성합니다.

1단계 **Policy > Authentication**으로 이동합니다.
2단계 매치할 **MAB** 규칙을 만듭니다.

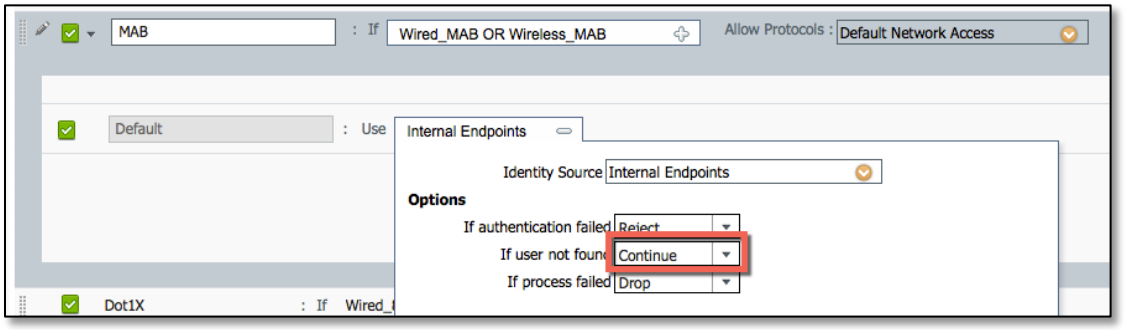

그림 5. MAB 규칙

3단계 **Guest Portal Sequence**를 변경하여 Active Directory 인스턴스를 포함합니다.
4단계 **Administration > Identity Source Sequence > Guest_Portal_Sequence**로 이동합니다.
5단계 AD 인스턴스를 오른쪽으로 이동합니다.

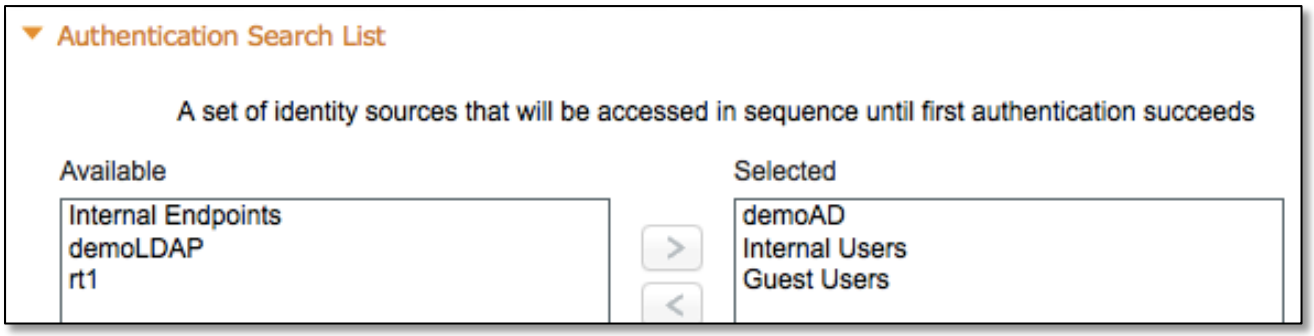

그림 6. 인증 검색 목록

권한 부여 프로필 생성

1단계 3가지 포털에 대한 **권한 부여 프로필**을 만듭니다.
2단계 **Policy > Results > Authorization > Authorization Profiles**로 이동합니다.

WLC-CWA, DRW_Apple, DRW_Microsoft의 3가지 프로필을 만듭니다.

WLC-CWA = 기본 사용자 지정 게스트 포털 리디렉션 프로필

업체 직원이 네트워크에 액세스할 때 처음으로 보는 포털입니다.

- Web Redirection에 Centralized Web Auth를 선택합니다.
- ACL "WLC-ACL_ISE-RESTRICTED"가 컨트롤러에 전달되며 이것이 리디렉션 ACL이 됩니다.
- Default_Custom은 사용자가 만든 포털입니다.

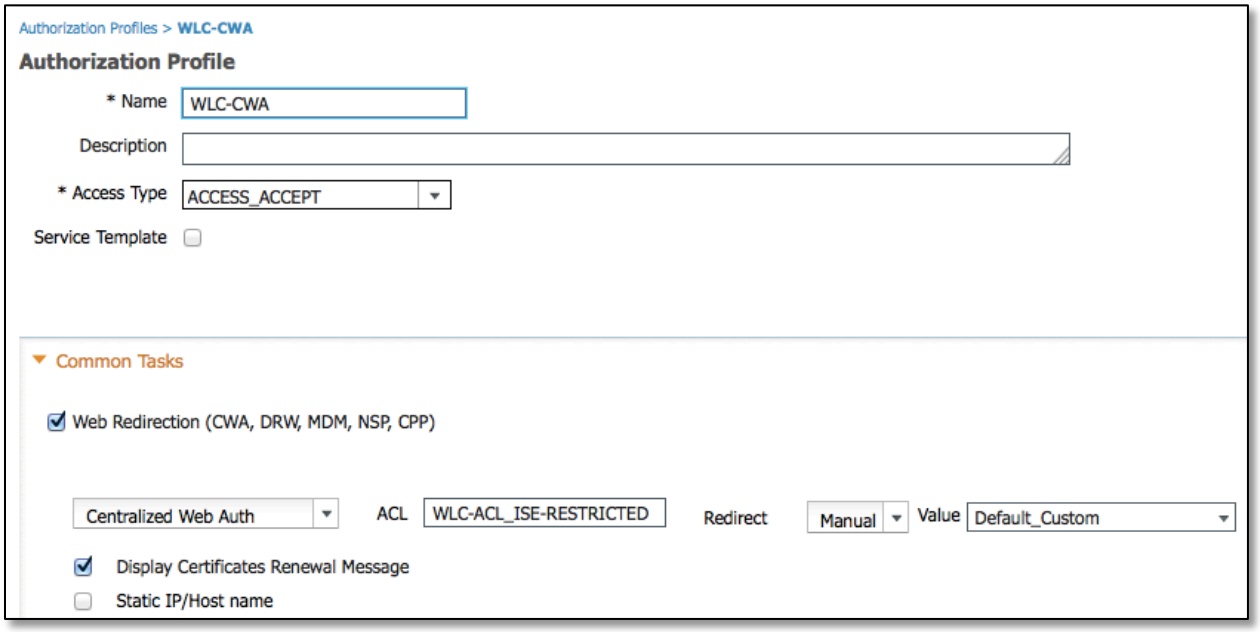

그림 7. 권한 부여 프로필 - WLC-CWA

DRW_Apple = Apple 업체 직원을 위한 DRW 정책

Apple 업체 직원이 CWA 포털에서 인증한 다음 리디렉션되는 포털입니다.

- Web Redirection에 Device Registration Web Auth를 선택합니다.
- ACL "WLC-ACL_ISE-RESTRICTED"가 컨트롤러에 전달되며 이것이 리디렉션 ACL이 됩니다.
- APPLE_DRW는 Apple 업체 직원의 DRW 성공을 위해 만든 포털입니다.

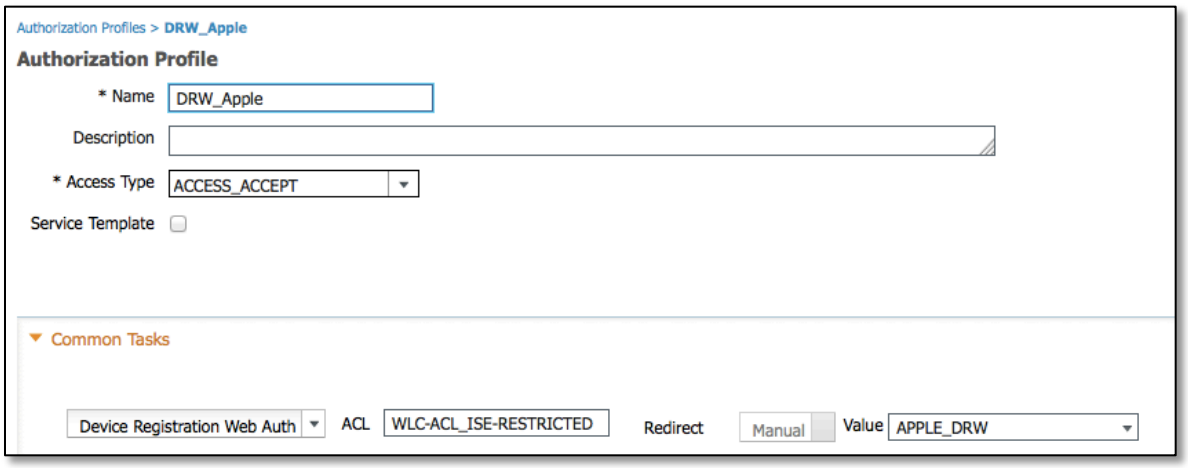

그림 8. 권한 부여 프로필 - DRW_Apple

DRW_Microsoft = Microsoft 업체 직원을 위한 DRW 정책

Microsoft 업체 직원이 CWA 포털에서 인증한 다음 리디렉션되는 포털입니다.

- Web Redirection에 Device Registration Web Auth를 선택합니다.
- ACL "WLC-ACL_ISE-RESTRICTED"가 컨트롤러에 전달되며 이것이 리디렉션 ACL이 됩니다.
- MICROSOFT_DRW는 MICROSOFT 업체 직원의 DRW 성공을 위해 만든 포털입니다.

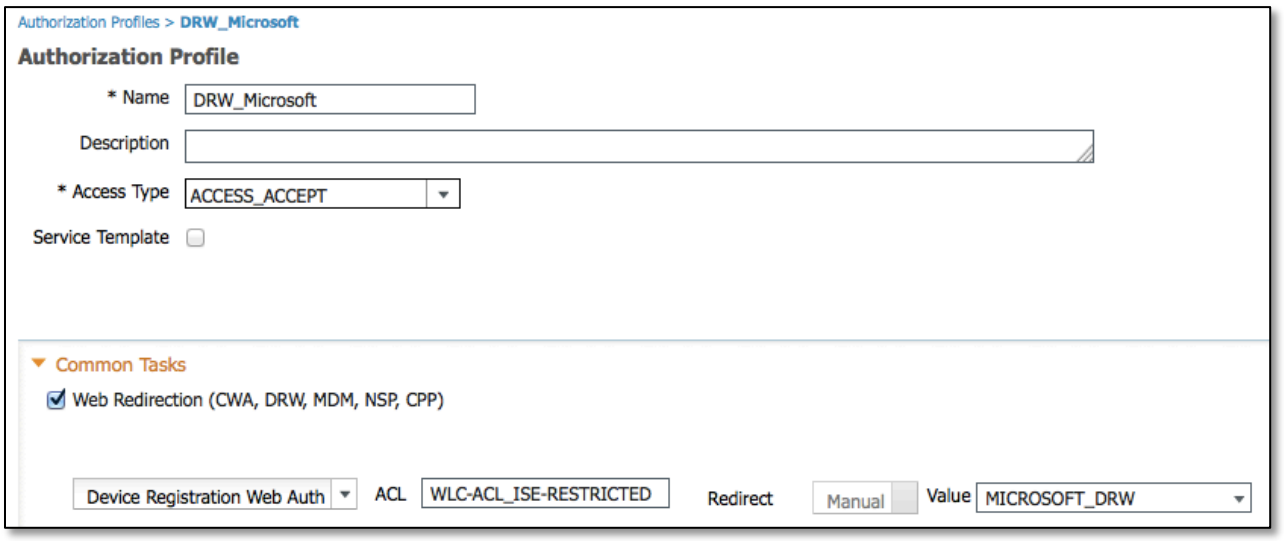

그림 9. 권한 부여 프로필 - DRW_Microsoft

권한 부여 정책 생성

마지막으로 아래의 설명 및 화면을 참조하여 권한 부여 정책을 만듭니다.

1단계 **Policy** > **Authorization**으로 이동합니다.

필수 조건은 아니지만 동일한 순서로 정책을 입력하는 것이 좋습니다.

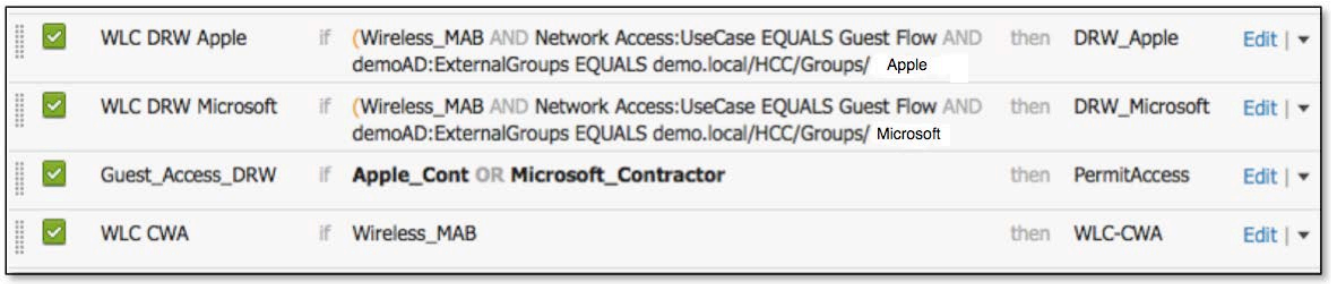

그림 10. 권한 부여 정책

WLC DRW Apple = 디바이스 등록을 위한 권한 부여 정책

Apple 업체 직원의 웹 인증에서는 다음 사항을 확인합니다.

- 디바이스가 무선에 연결되어 있음
- 디바이스가 앞서 WLC CWA 정책으로 인증되었으므로 아직 게스트 플로우에 있음
- 사용자는 AD 그룹 = Apple에 속해 있음

결과: 이 MAC 주소를 엔드포인트 ID 그룹 = Apple_*Contractor에 넣고 COA_Session_Terminate*를 실행합니다.

WLC DRW Microsoft = 디바이스 등록을 위한 권한 부여 정책

Microsoft 업체 직원의 웹 인증에서는 다음 사항을 확인합니다.

- 디바이스가 무선에 연결되어 있음
- 디바이스가 앞서 WLC CWA 정책으로 인증되었으므로 아직 게스트 플로우에 있음
- 사용자는 AD 그룹 = Microsoft에 속해 있음

결과: 이 MAC 주소를 엔드포인트 ID 그룹 = Microsoft_Contractor *에 넣고 COA_Session_Terminate*를 실행합니다.

Guest_Access_DRW = 권한 부여 정책

엔드포인트 ID 그룹에 따라 직원에게 액세스 권한을 부여하는 정책이며, Apple_Contractor와 Microsoft-Contractor에게 차별화된 액세스 권한을 부여하려는 경우 여러 정책으로 분할할 수도 있습니다.

엔드포인트 ID 그룹이 Apple_Contractor 또는 Microsoft_Contractor일 경우 PermitAccess

참고: 앞서 정의한 DRW 정책에 의해 MAC 주소가 이 엔드포인트 ID 그룹에 삽입되었습니다.

WLC CWA = 업체 직원이 로그인하도록 기본 사용자 지정 포털에 리디렉션

요약

사용자 경험을 요약하면 다음과 같습니다.

1단계 업체 직원이 개방형 무선 네트워크에 연결합니다.
2단계 디바이스가 웹 인증 포털에 리디렉션됩니다.
3단계 업체 직원이 자신의 AD 인증서로 로그인합니다.
4단계 성공 페이지가 표시되는 동안 다시 세션 권한 부여를 위해 COA가 전송됩니다.
5단계 성공 페이지에서는 자동으로 yahoo.com으로 이동하려 하고 다시 DRW 포털에 리디렉션됩니다.
6단계 DRW 포털에서 알맞은 그룹에 엔드포인트를 자동으로 등록하고 사용자 지정 성공 페이지를 표시합니다.
7단계 COA가 다시 수행되고 엔드포인트 그룹에서 디바이스 권한 부여가 이루어집니다.
8단계 다음 연결부터는 (엔드포인트가 해당 업체 직원 엔드포인트 그룹에서 지워지지 않는 한) 곧바로 액세스가 허용됩니다.

자세한 내용은 다른 방법 가이드를 참조하십시오.